CLAIMS

1. Data protection method (M) using, in a microprocessor of a chip card, a cryptographic algorithm for executing operations for processing data elements (M, M0, M1, M2, M3, K1, K2, K3, K4, K5, R1, R2, R3, R4, R5) so as to generate encrypted information (C), characterized in that it comprises at least one step for the random transformation (120) of bits of at least one of the data elements (K2) by associating a random number with said data element (K2) by means of a logical operator of the exclusive-OR type, and after this random transformation step, an inverse transformation step (220) such that the encrypted information (C) is unchanged by these transformation steps (120, 220).

2. Protection method according to claim 1, characterized in that a randomly transformed data element is a key (K1, K2, K3, K4, K5).

3. Protection method according to ~~either of claims 1 or 2~~ claim 1, characterized in that a randomly transformed data element is a message block (M, M0, M1, M2, M3).

4. Protection method according to ~~any of claims 1, 2 or 3~~ claim 1, characterized in that a randomly transformed data element is a message block associated with a key by a logical operator of the exclusive-OR type (R1, R2, R3, R4, R5).

5. Protection method according to ~~any of the preceding claims~~ claim 1, characterized in that the cryptographic algorithm for executing operations for processing data (M, M0, M1, M2, M3, K1, K2, K3, K4, K5, R1, R2, R3, R4, R5) comprises a group of operations (270) executed repeatedly.

6. Protection method according to claim 5, characterized

in that the random transformation step is a step that precedes the group of operations (270) executed repeatedly and in that the inverse transformation step is a step that follows said group of operations (270).

7. Protection method according to ~~any of the preceding claims~~ claim 1, characterized in that it also comprises a step for randomly modifying the order of execution of the operations of the group of operations (270).

8. Protection method according to ~~any of the preceding claims~~ claims 1, characterized in that the cryptographic algorithm is the DATA ENCRYPTION STANDARD type.